Тематическая статья
2.1. Теоретико-исторические правовые науки
УДК 342.31

ФОРМИРОВАНИЕ МЕХАНИЗМА ЦИФРОВОГО СУВЕРЕНИТЕТА РОССИИ КАК СТРАТЕГИЧЕСКОГО РЕСУРСА УКРЕПЛЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ (ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ)

FORMATION OF DIGITAL SUVEREIGNTY MECHANISMS IN RUSSIA AS A STRATEGIC RESOURCE FOR STRENGTHENING NATIONAL SECURITY IN THE CONTEXT (THEORETICAL AND LEGAL ANALYSIS)

Сведения об авторе:
Блинкова Виктория Александровна
Волгоградская академия МВД России,
Волгоград, Россия,
vblinkova2408@icloud.com,
https://orcid.org/0009-0005-2228-9137

Information about the author:
Blinkova Victoria Aleksandrovna
Volgograd Academy
of the Ministry of Internal Affairs of Russia,
Volgograd, Russia,
vblinkova2408@icloud.com,
https://orcid.org/0009-0005-2228-9137

Аннотация. Исследование посвящено теоретико-правовому анализу понятия цифрового суверенитета как стратегического ресурса укрепления национальной безопасности в Российской Федерации. Отмечается отсутствие однозначного понимания сущности и содержания цифрового суверенитета как в доктринальном, так и законодательном смыслах, что создает трудности в формировании эффективных правовых механизмов его обеспечения. Рассматриваются основные подходы ученых к формированию и реализации правотворческих механизмов цифрового суверенитета, направленных на защиту информационных ресурсов и суверенитета в цифровой сфере. Особое внимание уделяется иностранным цифровым платформам и инструментам защиты отечественных информационных сетей от негативного внешнего воздействия. Предлагается рассмотреть практику внедрения специализированных государственных услуг и платформ, таких как цифровой ID и портал «Госуслуги», в качестве основополагающих направлений к обеспечению цифрового суверенитета.
Ключевые слова: суверенитет, цифровой суверенитет, информационная безопасность, механизм, глобальная цифровизация, цифровые технологии, национальная безопасность.
Abstract. The study is devoted to the theoretical and legal analysis of the digital sovereignty concept as a strategic resource for strengthening national security in the Russian Federation. It is noted that there is no clear understanding of the essence and content of digital sovereignty, both in the doctrinal and legislative senses, which creates difficulties in developing effective legal mechanisms for ensuring digital sovereignty. The main approaches of scientists to the formation and implementation of legal mechanisms for digital sovereignty aimed at protecting information resources and sovereignty in the digital sphere are considered. Special attention is given to foreign digital platforms and tools for protecting domestic information networks from negative external influence. It is

proposed to consider the practice of implementing specialized public services and platforms, such as digital ID and the Gosuslugi portal, as fundamental approaches to ensuring digital sovereignty.
Keywords. Sovereignty, digital sovereignty, information security, mechanism, global digitalization, digital technologies, national security.

Ссылка для цитирования: Блинкова В. А. Формирование механизма цифрового суверенитета России как стратегического ресурса укрепления национальной безопасности (теоретико-правовой анализ) // Трактат правовых инициатив. 2026.

For citation: Blinkova V. A. Formation of Digital Sovereignty Mechanism in Russia as a Strategic Resource for Strengthening National Security (Theoretical and Legal Analysis). Journal of Legal Initiatives, 2026. (In Russ.).

ВВЕДЕНИЕ

В условиях глобальной цифровизации и активного развития цифровых технологий во всех сферах общественной жизни в научный дискурс вошло понятие «цифровой суверенитет». Его возникновение обусловлено объективной необходимостью переосмысления новых форм реализации государственного суверенитета в цифровой среде, характеризующейся трансграничным характером данных, появлением глобальных цифровых платформ и высокой степенью технологической зависимости государств друг от друга. Обретение и укрепление цифрового суверенитета – одна из важнейших функций государства в цифровую эпоху[1]. М. М. Кучерявый убежден, что «цифровой суверенитет есть верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации Pravo.gov.ru. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 29.01.2026).

глобальном информационном пространстве» [1, с. 12]. Однако в настоящее время отсутствует общепринятое определение данного понятия.

МЕТОДЫ

При производстве исследования были использованы следующие методы:

– структурно-функциональный метод, позволяющий детально рассмотреть формирование и реализацию механизмов цифрового суверенитета как систему взаимосвязанных элементов и определить назначение каждого из них;

– системный метод позволил рассмотреть цифровой суверенитет как целостную, многоуровневую и динамическую систему, состоящую из взаимосвязанных подсистем;

– сравнительно-правовой метод позволил рассмотреть различные подходы к определению «цифровой суверенитет».

РЕЗУЛЬТАТЫ

Развитие цифровых технологий и формирование цифрового пространства привели к возникновению совершенно новых общественных отношений, которые выходят за государственные границы. В научных изысканиях указывается, что цифровая среда существенно ослабляет традиционные механизмы территориального контроля, что требует адаптации функций суверенного государства к новым информационным условиям.

В отечественной правовой доктрине идея цифрового суверенитета зародилась в начале 2000-х гг. Обусловлено это появлением новой концепции суверенитета данных, направленной на установление информационного контроля над персональными данными как физических, так и юридических лиц, находящихся на территории Российской Федерации. По мнению ряда ученых, «цифровой суверенитет рассматривается как возможность государства контролировать свои

цифровые данные, информацию, а также обеспечивать безопасность и защиту цифровых технологий и инфраструктуры» [2, с. 4]. Думается, что это понятие не ограничивается лишь техническими параметрами цифровых технологий, а включает в себя широкий спектр политических, экономических и социальных аспектов.

Признаки цифрового суверенитета государства обусловлены наличием автономных, высокопроизводительных и конкурентоспособных программных решений, позволяющих эффективно выполнять разнообразные задачи, включая создание национальных операционных систем, инструментов обработки больших объемов данных, систем мониторинга, анализа и прогнозирования, а также разработку технических сервисов в сфере искусственного интеллекта. В указанном контексте особую важность приобретают технологический потенциал государства и степень его независимости от зарубежных поставщиков высокотехнологичной продукции.

В свою очередь, следует разграничивать термины «цифровой» и «информационный» суверенитет. А. В. Россошанский убежден, что «информационный суверенитет – это способность и намерение субъекта политики производить и распределять информацию в зависимости от собственных интересов и использовать информацию как ресурс политического влияния в масштабах и объемах, которые соответствуют его текущим и долгосрочным политическим интересам» [3, с. 185], тогда как А. А. Ефремов считает, что «цифровой суверенитет определяется через самостоятельную способность создавать, хранить, распространять и потреблять информацию» [4, с. 58].

Несмотря на то что в настоящее время термин «цифровой суверенитет» широко употребляется в научном сообществе, его законодательное закрепление до сих пор отсутствует, что обусловлено сложностью его интеграции в нормативно-правовую систему государства.

Развитие цифрового суверенитета посредством создания новых механизмов его регулирования является стратегически важной задачей, способствующей укреплению национальной безопасности государства. Правовое регулирование отдельных видов цифровых правоотношений в российской сети Интернет осуществляется специализированным государственным органом – Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором). Как отмечает Н. А. Троян, «в современных реалиях не всегда данное явление проявляет устойчивость перед новыми вызовами» [5, с. 170]. Это подтверждается неудавшейся попыткой, предпринятой в 2018 г. Роскомнадзором, который стремился запретить доступ к мессенджеру Telegram вследствие отказа владельцев ресурса предоставить уполномоченным органам ключи криптографического доступа к сообщениям пользователей. Итогом стало мгновенное ограничение доступа российских граждан примерно к 18 млн IP-адресов, что негативно сказалось на работе других интернет-сервисов и подтолкнуло значительную часть пользователей к применению VPN и прокси-серверов для обхода блокировки.

Из-за начавшейся информационной войны западных политических кругов в цифровом пространстве против России, стартовавшей сразу после начала специальной военной операции, российское государство было вынуждено принять меры по ограничению доступа к ряду зарубежных онлайн-платформ, включая Instagram, WhatsApp и Facebook (признаны экстремистскими организациями, деятельность которых на территории Российской Федерации запрещена). Эти ресурсы систематически игнорировали как внутренние правила функционирования собственных платформ, так и действующее законодательство нашей страны. Несмотря на то, что технически каждый пользователь способен обойти подобные ограничения посредством специальных инструментов, определенный

положительный результат от действий государства наблюдался: за первый год после введения блокировок объем трафика из России на указанные ресурсы сократился многократно. Тем не менее это лишь малая часть масштабных задач и серьезных проблем, стоящих перед страной в сфере защиты своего цифрового суверенитета, ввиду отсутствия законодательно установленной правовой конструкции.

Как отмечает А. С. Агафонов, «цифровой суверенитет – это правовой институт, т. е. система норм права, регулирующих обособленные общественные отношения, связанные с обеспечением самостоятельности реализации публичных государственных функций в области создания и применения наукоемких информационных технологий, критически важных для обеспечения независимости и конкурентоспособности» [6, с. 15]. Важное место занимают правовые механизмы, которые включают в себя нормативно-правовое регулирование. Формирование цифрового суверенитета в Российской Федерации осуществляется преимущественно посредством издания правотворческих актов, закрепляющих основы государственной политики в цифровой сфере и определяющих правовые механизмы защиты национальных интересов. Именно нормативно-правовое регулирование выступает ключевым инструментом институционализации цифрового суверенитета, придавая ему системный характер. Важно подчеркнуть, что право является основным средством выражения суверенной воли государства, в том числе в цифровой среде, поскольку именно через правовые нормы государство устанавливает пределы допустимого поведения субъектов цифровых отношений и механизмы контроля над ними. В этой связи правотворческая деятельность государства приобретает особую значимость. Базовые положения, отражающие элементы цифрового суверенитета, закреплены в стратегических документах Российской Федерации. Так, согласно Указу Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной

безопасности Российской Федерации»[1] цифровая сфера воспринимается в качестве ключевого фактора укрепления национальной безопасности, а обеспечение защиты информационных и технологических ресурсов определяется в качестве стратегического приоритета государства.

Другим значимым документом, способствующим формированию цифрового суверенитета, является Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[2], в которой прямо указывается на необходимость обеспечения технологической независимости, устойчивости национальной информационной инфраструктуры и защиты цифрового пространства от внешнего воздействия. В данном документе не употребляется термин «цифровой суверенитет», однако соответствующие положения, закрепленные в Доктрине, отражают процесс обеспечения государственно-правового регулирования в информационной сфере. Документ предполагает, что информационная безопасность – это состояние защищенности личности, общества, государства от внутренних и внешних информационных угроз, при котором обеспечивается реализация первостепенных конституционных прав и свобод человека и гражданина, достойное качество жизни, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Под цифровым суверенитетом можно понимать компонент общенациональной безопасности, направленный на обеспечение независимости и

[1] О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 2 июля 2021 г. № 400 // Официальный интернет-портал правовой информации Pravo.gov.ru. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 29.01.2026).

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации Pravo.gov.ru. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 29.01.2026).

устойчивости функционирования информационной инфраструктуры, защиты стратегических ресурсов и информационных прав субъектов.

Не менее значимым нормативным правовым актом является Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1], направленный на обеспечение устойчивости и защищенности значимых объектов цифровой инфраструктуры, что рассматривается в научной литературе как необходимое условие сохранения управляемости государства в цифровой сфере.

Правовой контроль над данными выступает одним из ключевых инструментов защиты цифрового суверенитета государства. В этой связи значимость приобретает Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[2], целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных. Последние в условиях цифровизации приобретают значение стратегического ресурса, влияющего в том числе на национальную безопасность Российской Федерации. А. П. Кочетков и К. В. Маслов подчеркивают, что «цифровизация, с одной стороны, предполагает новые возможности для социального, экономического развития, а с другой стороны, представляет собой вызов для национальной безопасности» [7, с. 35].

В условиях глобализации цифрового пространства и транснационального характера информационных потоков особое значение для обеспечения цифрового суверенитета приобретает правовое

[1] О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. № 187-ФЗ // Официальный интернет-портал правовой информации Pravo.gov.ru. URL: http://www.kremlin.ru/acts/bank/42128 (дата обращения: 29.01.2026).

[2] См.: О персональных данных: федер. закон от 27 июля 2006 г. № 152-ФЗ // Официальный интернет-портал правовой информации Pravo.gov.ru. URL: http://www.kremlin.ru/acts/bank/24154 (дата обращения: 30.01.2026).

регулирование деятельности иностранных цифровых платформ и информационных ресурсов, влияющих на общественные отношения внутри государства. По мнению ряда ученых, «взаимодействие с международными интернет-компаниями строится на основе соблюдения российских нормативных требований, направленных на защиту прав граждан, обеспечение законности и информационной безопасности» [8, с. 7]. Следует обратить особое внимание на то, что важную роль в системе правового регулирования интернет-пространства получила концепция «приземления» иностранных IT-компаний, регулируемая Федеральным законом от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети „Интернет“ на территории Российской Федерации»[1]. Нормативный правовой акт имеет публично-правовую направленность и ориентирован на преодоление экстерриториального характера деятельности иностранных цифровых платформ. Р. С. Нерсесян уверен, что «федеральный закон является механизмом по формированию цифрового суверенитета в Российской Федерации, который не только обеспечивает контроль над иностранными цифровыми платформами, деятельность которых затрагивает интересы российских пользователей, но и способствует снижению зависимости национального информационного пространства от внешних цифровых и инфраструктур» [9, с. 25], поэтому концепцию «суверенитета данных» можно считать обоснованной и верной. В то же время Е. В. Алферова отмечает, что «фрагментарность нормативного регулирования цифрового суверенитета во многом предопределена отсутствием системности в осмыслении данной категории на научно-доктринальном уровне» [10, с. 184].

[1] О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации: федер. закон от 1 июля 2021 г. № 236-ФЗ // Официальный интернет-портал правовой информации Pravo.gov.ru. URL: http://www.kremlin.ru/acts/bank/46991 (дата обращения: 30.01.2026).

Национальная безопасность Российской Федерации – состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качества и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны[1]. По мнению А. В Маилян, «национальная безопасность представляет собой систему различных видов безопасности» [11, с. 65]. К таковым можно отнести и информационную безопасность, являющуюся узловым элементом цифрового суверенитета. В научных трудах подчеркивается, что способность государства управлять информационным пространством и минимизировать угрозы цифрового характера напрямую влияет на эффективность обеспечения национальной безопасности. В этом контексте информационный суверенитет рассматривается как инструмент, который позволяет государству сохранять самостоятельность в управлении информационными процессами, поддерживать устойчивость государственных институтов и предотвращать негативное воздействие внешних и внутренних угроз. Стоит отметить, что укрепление информационного суверенитета выступает не только как условие защиты национальных интересов, но и как необходимый элемент стратегического обеспечения национальной безопасности. Это создает прочную основу для дальнейшего формирования механизмов цифрового суверенитета, которые в современных условиях становятся ключевым инструментом защиты государства в цифровой сфере.

[1] О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 2 июля 2021 г. № 400 // Официальный интернет-портал правовой информации Pravo.gov.ru. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 30.01.2026).

Тем не менее термин «цифровой суверенитет» пока не закреплен в нормативных правовых актах, что создает неопределенность в правоприменении и ограничивает эффективность существующих механизмов. В современных условиях цифровизации, когда информационные и технологические ресурсы приобретают стратегическое значение, необходимо законодательное закрепление данного понятия. Его формирование через систему нормативных правовых актов при условии законодательного закрепления и унификации терминологии позволит государству эффективно противодействовать современным цифровым угрозам, сохранять независимость в управлении информационными процессами. Практические механизмы реализации цифрового суверенитета включают создание государственных цифровых платформ и сервисов, ориентированных на соответствие национальным интересам и стандартам безопасности. Примером может служить многофункциональный сервис обмена информацией, который упростил оформление документов и расширил возможности электронного документооборота для граждан. Ключевым компонентом указанного сервиса выступает цифровой идентификатор (ID), выполняющий функцию электронного документа, удостоверяющего личность. В мобильное приложение встроено средство «Госключ», предназначенное для электронной подписи документов, а также обеспечивающее защищенный обмен информацией среди пользователей, прошедших процедуру идентификации и аутентификации. Создание такой платформы обмена данными – важный шаг к цифровому суверенитету России. По словам Президента РФ В. В. Путина, «информационная независимость невозможна при зависимости от иностранных платформ, которые могут быть отключены в любой момент»[1]. Единая система межведомственного

[1] Путин: у РФ не будет информационной независимости без собственных интернет-платформ. URL: https://tass.ru/ekonomika/10285417 (дата обращения: 02.02.2026).

электронного взаимодействия и другие государственные цифровые реестры, которые обеспечивают централизованный контроль над критической цифровой информацией, повышают прозрачность и защищают данные граждан. Эти платформы, функционирующие в рамках государственной политики цифровизации, способствуют укреплению управляемости цифровыми процессами и минимизации зависимости от иностранных технологических решений. Е. А. Зевелева и К. А. Кокунов высказывают точку зрения, заключающуюся в том, что «формирование цифрового суверенитета России является стратегической задачей, решение которой позволит обеспечить ее политическую и экономическую безопасность» [12, с. 93].

ЗАКЛЮЧЕНИЕ

Проведенный анализ позволяет сделать вывод о том, что формирующийся цифровой суверенитет в Российской Федерации выступает объективно необходимым элементом реализации государственного суверенитета и неотъемлемой составляющей системы национальной безопасности государства. Глобальная цифровизация, трансграничный характер информационных потоков и возрастающая роль цифровых платформ, в том числе иностранных, требуют формирования правовых механизмов регулирования в цифровой среде. На сегодняшний день в Российской Федерации сложилась фрагментарная, но поступательно развивающаяся система нормативно-правового регулирования, направленная на формирование цифрового суверенитета, а стратегические документы и федеральные законы в сфере информационной безопасности фактически формируют институциональную основу данного термина, несмотря на отсутствие его законодательного определения. Указанные правовые акты закрепляют приоритет национальных интересов, технологической независимости и контроля над ключевыми цифровыми ресурсами, что свидетельствует о признании цифровой сферы

стратегически значимой для государства. Вместе с тем отсутствие нормативно закрепленного понятия «цифровой суверенитет» и единой концепции его реализации порождает правовую неопределенность и снижает эффективность правоприменительной практики. Существующие меры носят преимущественно реактивный характер и не всегда сопровождаются системным правовым и технологическим обеспечением, что наглядно демонстрируют отдельные примеры регулирования деятельности цифровых платформ и ограничения доступа к зарубежным сервисам.

В условиях нарастания цифровых угроз и усиления внешнего информационного воздействия особую значимость приобретает дальнейшее формирование правовых механизмов цифрового суверенитета, включая законодательное закрепление данного понятия и выработку комплексной государственной политики в цифровой сфере. О. В. Романовская убеждена, что «концепция цифрового суверенитета – ответная реакция государства на те угрозы, которые оно ощущает благодаря отчасти неконтролируемому развитию ИКТ» [13, с. 181].

Таким образом, цифровой суверенитет следует рассматривать не как абстрактную доктринальную категорию, а как практико-ориентированный правовой институт, направленный на защиту национальных интересов, обеспечение информационной безопасности и сохранение самостоятельности государства в условиях глобальной цифровой трансформации. В подтверждение следует привести цитату А. К. Дубеня, который считает, что «цифровой суверенитет является возможностью независимого суверенного государства самостоятельно определять степень и способ участия в информационной деятельности при применении цифровых технологий для реализации собственных интересов и противодействия противоправным действиям в национальном информационном пространстве» [14, с. 90]. Обеспечение цифрового

суверенитета Российской Федерации является необходимым условием сохранения государством своей конкурентоспособности и укрепления национальной безопасности в современном информационно-технологическом пространстве. Цифровой суверенитет предполагает реализацию комплекса правовых, организационных и технических мероприятий, направленных на предотвращение негативного воздействия извне, защиту национальных информационных ресурсов, минимизацию рисков распространения дезинформации и манипулирования общественным мнением путем формирования эффективной системы контроля над цифровым пространством и обеспечения информационной безопасности граждан.

Российская Федерация, несмотря на отставание в отдельных секторах «высоких технологий», демонстрирует высокий уровень развития в области разработки программного обеспечения и подготовки квалифицированных кадров в сфере информационных технологий. Государственными органами осуществляется поддержка отечественного сектора цифровых технологий, включая предоставление финансовой помощи российским IT-предприятиям, что обеспечивает благоприятные правовые условия для реализации инновационной деятельности, и в этой связи нельзя не согласиться с мнением Д. А. Карева, который считает, что «самым важным в построении цифрового суверенитета является постоянное движение вперед, создание передовых производств и подготовка высококвалифицированных кадров» [15, с. 83].

СПИСОК ИСТОЧНИКОВ

1. Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2014. № 9 (69). С. 7–14.

2. Авдийский В. И., Иванов А. В., Царегородцев А. В. Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы // Вестник евразийской науки. 2024. № 3. С. 1–19.

3. Россошанский А. В. Политический и информационный суверенитет в контексте процессов глобализации // Симбирский научный вестник. 2011. № 4 (6). С. 154–185.

4. Ефремов А. А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т. 63, № 1. С. 47–61.

5. Троян Н. А. Правовое обеспечение цифрового суверенитета России: актуальные проблемы и перспективные направления // Право и государство: теория и практика. 2024. № 6 (234). С. 169–172.

6. Агафонов А. С. Место цифрового суверенитета в системе информационного права // Электронное приложения к Российскому юридическому журналу. 2024. № 2. С. 14–18.

7. Кочетков А. П., Маслов К. В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Политические науки. 2022. № 2. С. 31–45.

8. Романовская Л. Р., Колесов М. С. Феномен цензуры в интернете со стороны глобальных цифровых платформ. Анализ иностранного опыта правового регулирования // Human Progress. 2025. Том 11, № 4. С. 1–16.

9. Нерсесян Р. С. Доктрина Когнитивно-технологического суверенитета в цифровую эпоху // Universum: общественные науки. 2025. № 11 (126). С. 23–32.

10. Алферова Е. В. Государственный суверенитет в информационном (цифровом) пространстве: доктринальные и законодательные подходы //

Социальные и гуманитарные науки. Отечественная и зарубежная литература. 2024. № 2. С. 171–186.

11. Маилян А. В. Национальная безопасность: анализ проблем // Право и государство: теория и практика. 2024. № 8 (236). С. 62–65.

12. Зевелева Е. А. Кокунов К. А. Информационный суверенитет России в эпоху цифровых технологий // Человек. Общество. Инклюзия. 2024. №2. 2024. Т. 15, № 2. С. 89–96.

13. Романовская О. В. Право, информационное общество, цифровой суверенитет // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2024. №2. С. 174–183.

14. Дубень А. К. Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации: дис. ... канд. юрид. наук. Москва, 2023. 239 с.

15. Карев Д. А. Цифровой суверенитет // Право и государство: теория и практика. 2025. № 4. С. 80–83.

REFERENCES

1. Kucheryavy`j M. M. Gosudarstvennaya politika informacionnogo suvereniteta Rossii v usloviyax sovremennogo global`nogo mira // Upravlencheskoe konsul`tirovanie. 2014. № 9 (69). S. 7–14.

2. Avdijskij V. I., Ivanov A. V., Czaregorodcev A. V. Vzaimosvyaz` cifrovogo suvereniteta i cifrovogo prostranstva: novy`e vy`zovy` i perspektivy` // Vestnik evrazijskoj nauki. 2024. № 3. S. 1–19.

3. Rossoshanskij A. V. Politicheskij i informacionny`j suverenitet v kontekste processov globalizacii // Simbirskij nauchny`j vestnik. 2011. № 4 (6). S. 154–185.

4. Efremov A. A. Gosudarstvenny`j suverenitet v usloviyax cifrovoj transformacii // Pravovedenie. 2019. T. 63, № 1. S. 47–61.

5. Troyan N.A. Pravovoe obespechenie cifrovogo suvereniteta Rossii: aktual`ny`e problemy` i perspektivny`e napravleniya // Pravo i gosudarstvo: teoriya i praktika. 2024. № 6 (234). S. 169–172.

6. Agafonov A. S. Mesto cifrovogo suvereniteta v sisteme informacionnogo prava // E`lektronnoe prilozheniya k Rossijskomu yuridicheskomu zhurnalu. 2024. № 2. S. 14–18.

7. Kochetkov A. P., Maslov K. V. Cifrovoj suverenitet kak osnova nacional`noj bezopasnosti Rossii v global`nom cifrovom obshhestve // Vestnik Moskovskogo universiteta. Politicheskie nauki. 2022. № 2. S. 31–45.

8. Romanovskaya L. R., Kolesov M. S. Fenomen cenzury` v internete so storony` global`ny`x cifrovy`x platform. Analiz inostrannogo opy`ta pravovogo regulirovaniya // Human Progress. 2025. T. 11, № 4. S. 1–16.

9. Nersesyan R. S. Doktrina Kognitivno-texnologicheskogo suvereniteta v cifrovuyu e`poxu // Universum: obshhestvenny`e nauki. 2025. № 11 (126). S. 23–32.

10. Alferova E. V. Gosudarstvenny`j suverenitet v informacionnom (cifrovom) prostranstve: doktrinal`ny`e i zakonodatel`ny`e podxody` // Social`ny`e i gumanitarny`e nauki. Otechestvennaya i zarubezhnaya literatura. 2024. № 2. S. 171–186.

11. Mailyan A. V. Nacional`naya bezopasnost`: analiz problem // Pravo i gosudarstvo: teoriya i praktika. 2024. № 8 (236). S. 62-65.

12. Zeveleva E. A. Kokunov K. A. Informacionny`j suverenitet Rossii v e`poxu cifrovy`x texnologij // Chelovek. Obshhestvo. Inklyuziya. 2024. №2. 2024. T. 15, № 2. S. 89–96.

13. Romanovskaya O. V. Pravo, informacionnoe obshhestvo, cifrovoj suverenitet // Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya: E`konomika. Upravlenie. Pravo. 2024. T. 24, № 2. S. 174–183.

14. Duben` A. K. Pravovoe obespechenie informacionnoj bezopasnosti v sisteme informacionnogo prava v Rossijskoj Federacii: dis. ... kand. yurid. nauk. Moskva, 2023. 239 s.

15. Karev D. A. Cifrovoj suverenitet // Pravo i gosudarstvo: teoriya i praktika. 2025. № 4. S. 80–83.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником; не содержит сведения, составляющие государственную и иную охраняемую законом тайну, информацию, предназначенную для служебного пользования; ранее не публиковался и в настоящее время не находится на предмет публикации в других изданиях.

09.02.2026 _____ В.А. Блинкова
(подпись)

Текст согласован с научным руководителем.

Научный руководитель
профессор кафедры конституционного и административного права
Волгоградской академии МВД России
д.ю.н., доцент Н.И. Грачев